


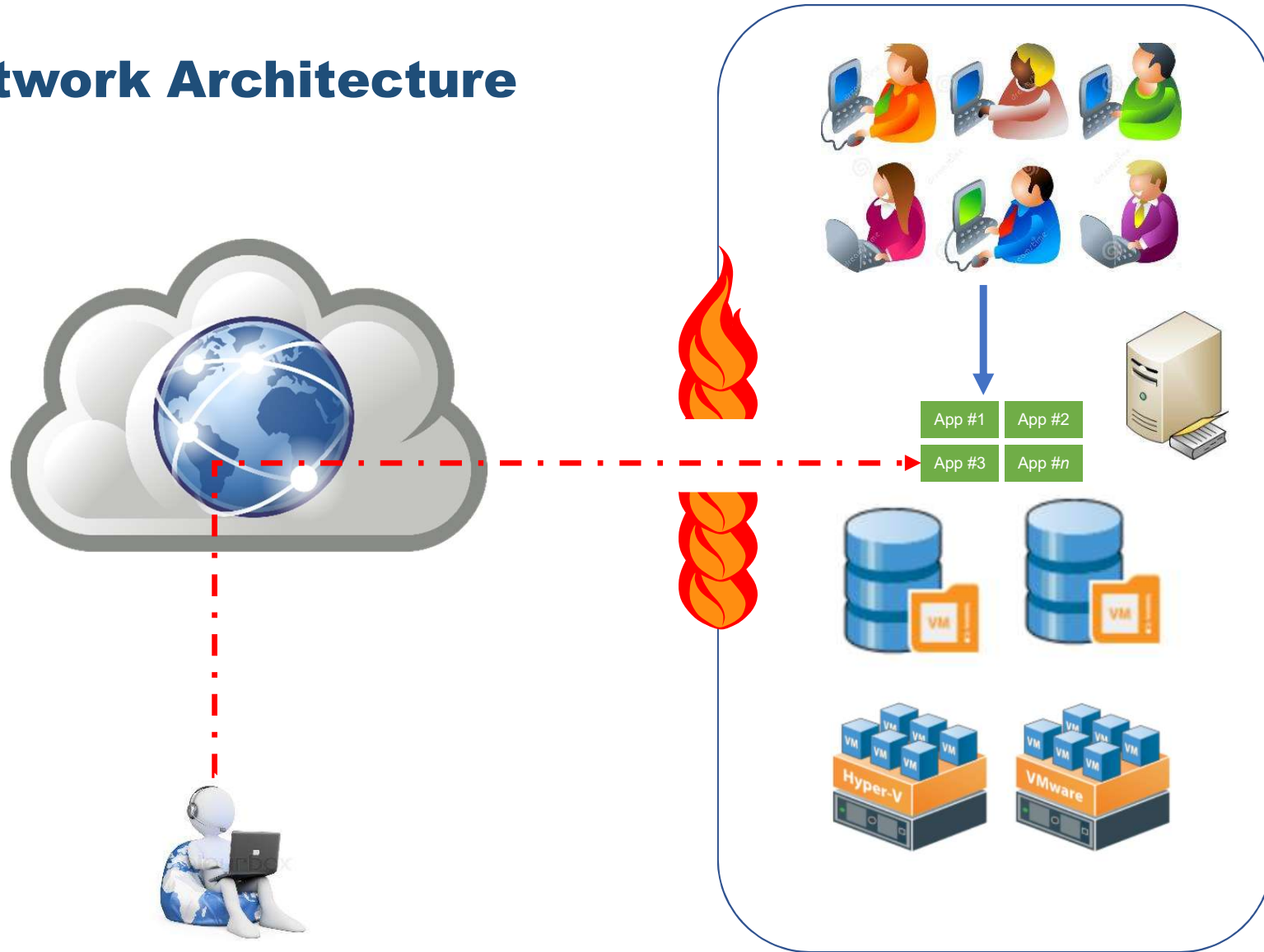
# Is your security model evolving?

Douglas Holland, CISSP  
Solutions Engineer-Akamai

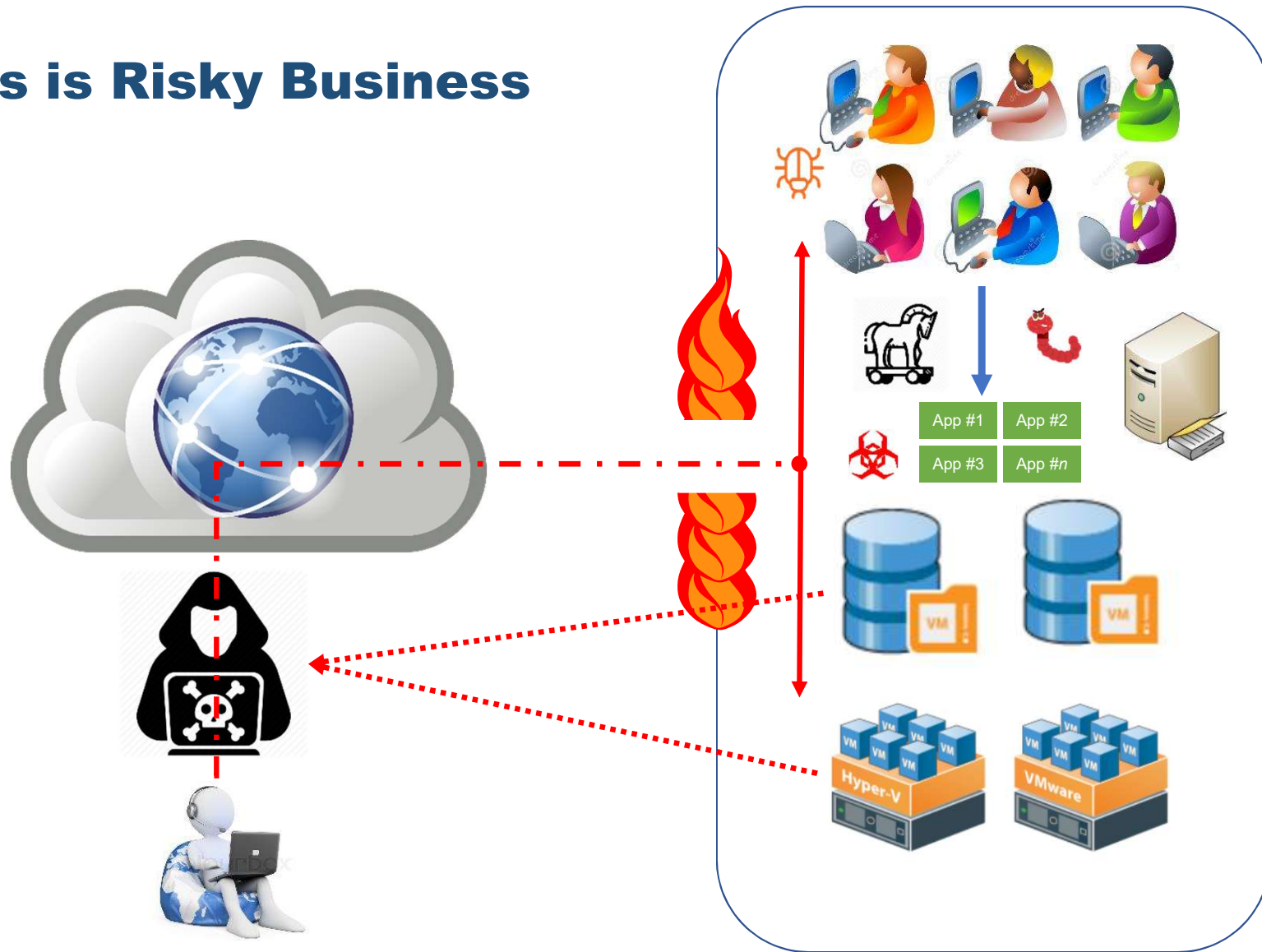
# Today I'll talk about:

- 
- How networks are architected today
  - Why this bad
  - What is a possible solution
  - Strategies to implement this solution
  - Case Study

# Traditional Network Architecture



# Remote Access is Risky Business



# Why Traditional VPN Elimination?

*“DMZs and legacy VPNs were designed for the networks of the 1990s and have become obsolete because they lack the agility needed to protect digital businesses.”*



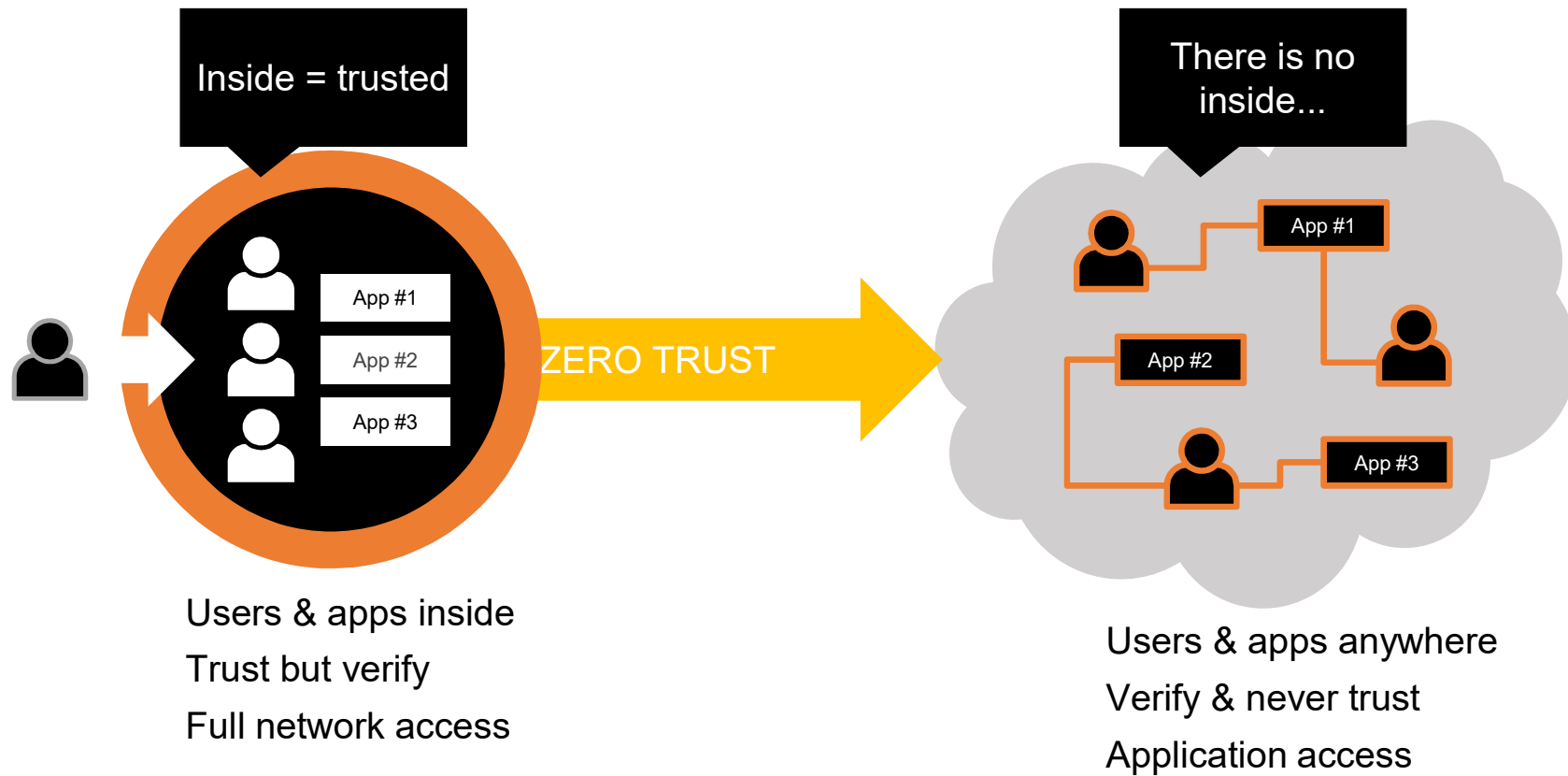


*The idea of a corporate perimeter is quaint – even dangerous*  
**Bottom line:** security perimeters belong in the past

# Users & Corporate Apps Have Left the Building!



# Cloud Requires Security Evolution





# What's Zero Trust?

## Key principles:

- Assume a hostile environment
- Don't distinguish between external & internal
- Never trust and only deliver applications/data to authenticated & authorized users/devices
- Always verify with logging & behavioral analytics



# Why Zero Trust Security Transformation?

*“Legacy perimeter security simply won’t work and won’t scale for the requirements of digital business and digital government. Digital transformation inverts our entire security model, further increasing the risk of legacy network security models.”*

# Strategies for Implementing Zero Trust



**Option 1: Network Segmentation**

**Option 2: Software Defined Perimeter**

**Option 3: Identity Aware Proxy**

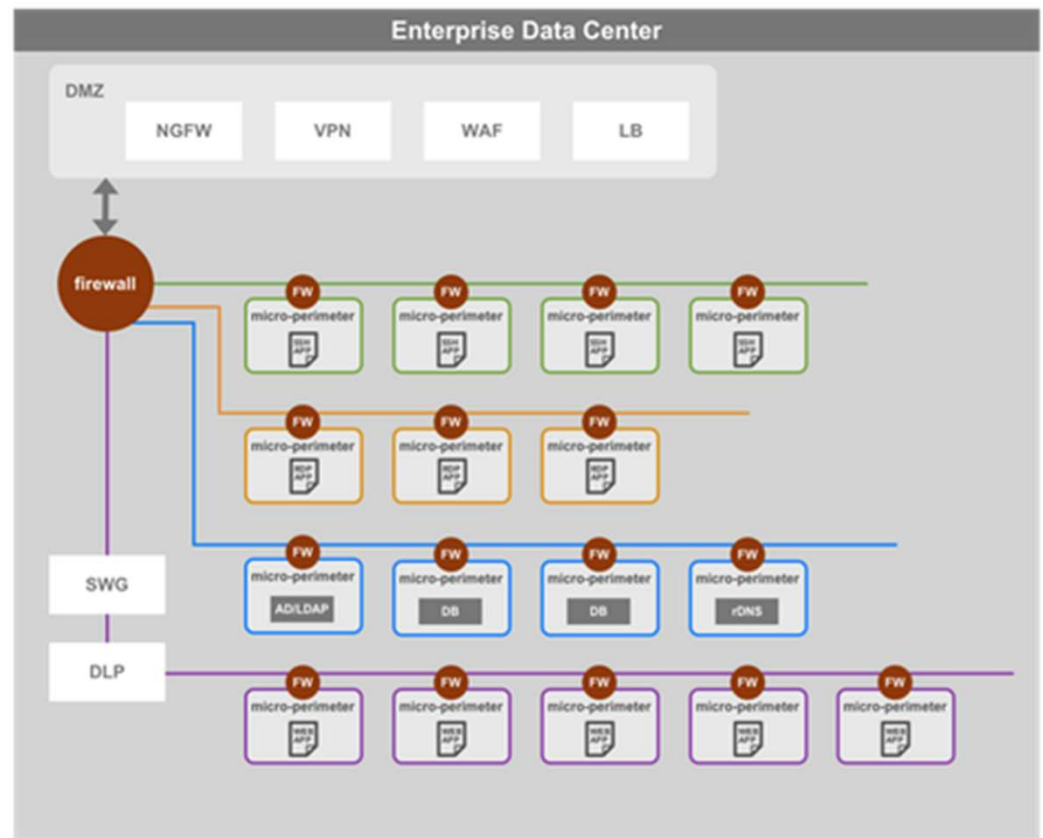
# Network Micro-Segmentation

- Pros

- Small Logical Networks
- Only allow the minimum needed service

- Cons

- Must define security zones tightly
- Maintenance/Complexity





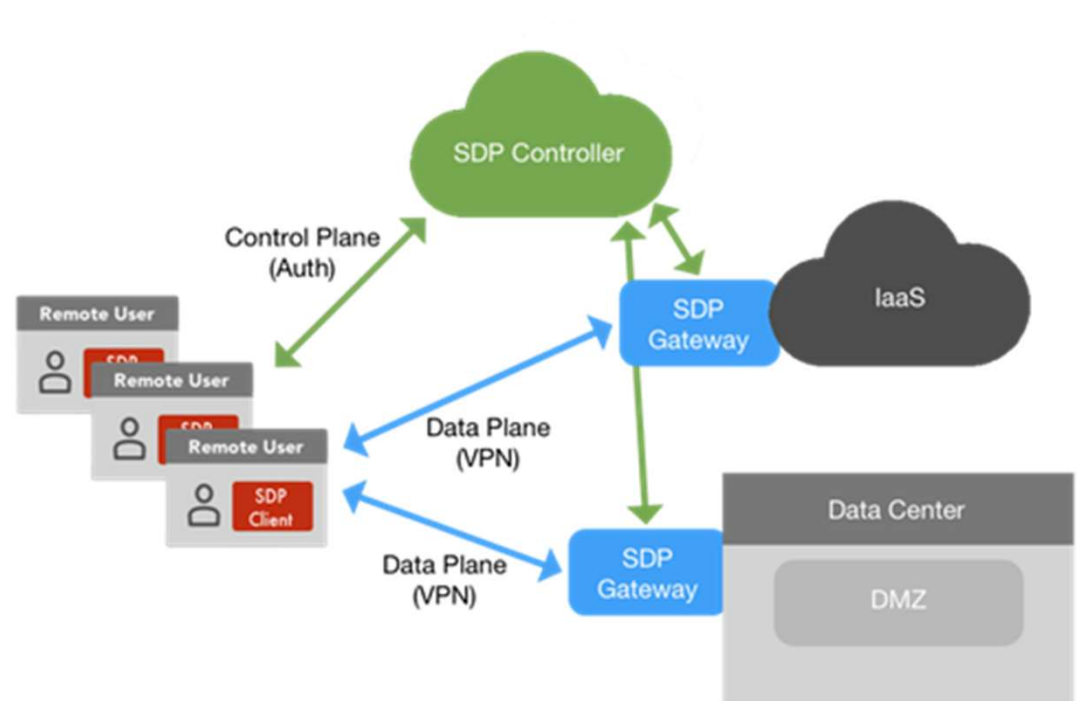
# Software Defined Perimeters

- Pros

- Unique tunnel for the service
- Data and Control plane separate

- Cons

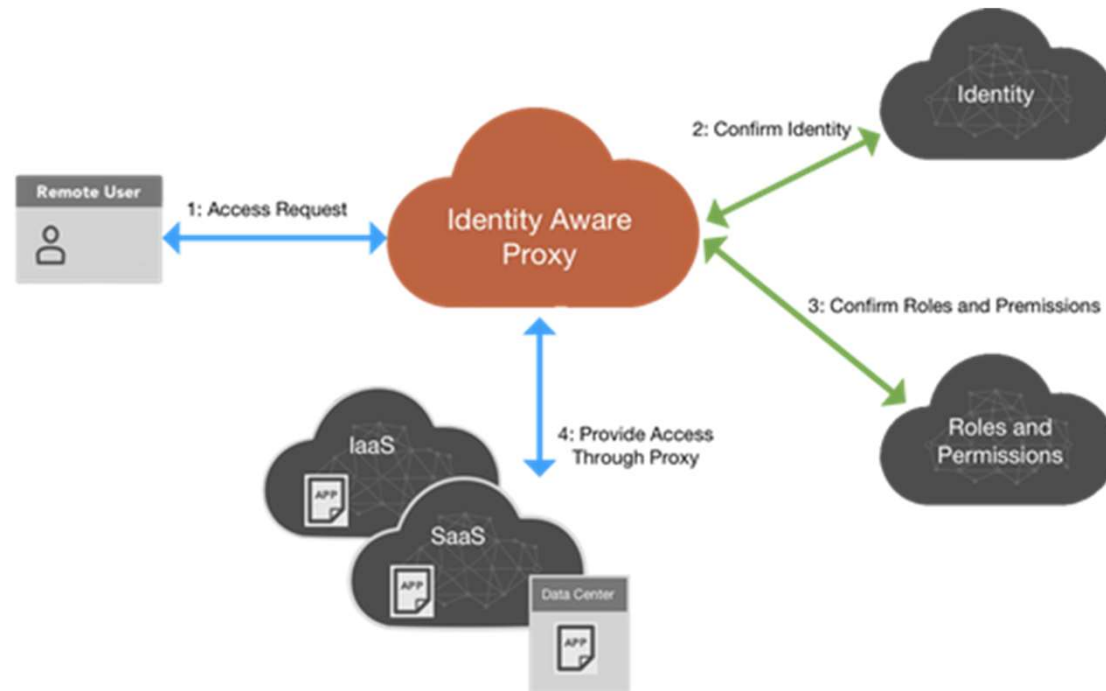
- Typically requires a client
- No termination within tunnel for additional services



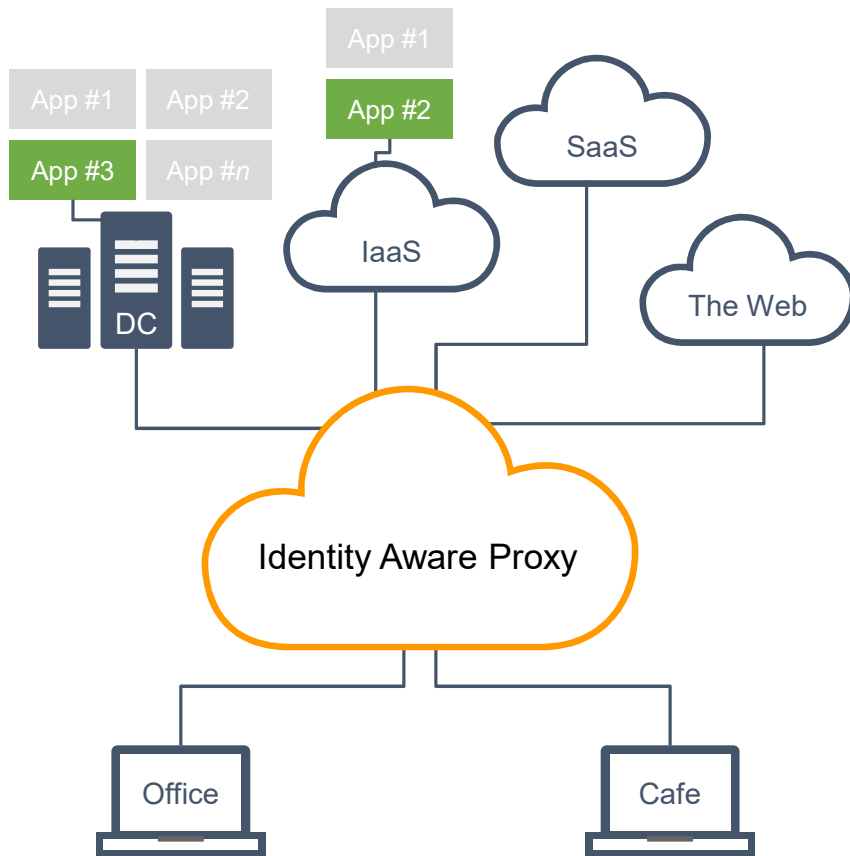
# Identity Aware Proxies

- Pros

- Layer 7 Proxy
- Application requests can be terminated, examined, and authorized
- Clientless and Client Access



# Adaptive Access & Threat Protection



One edge platform to secure all enterprise apps & users

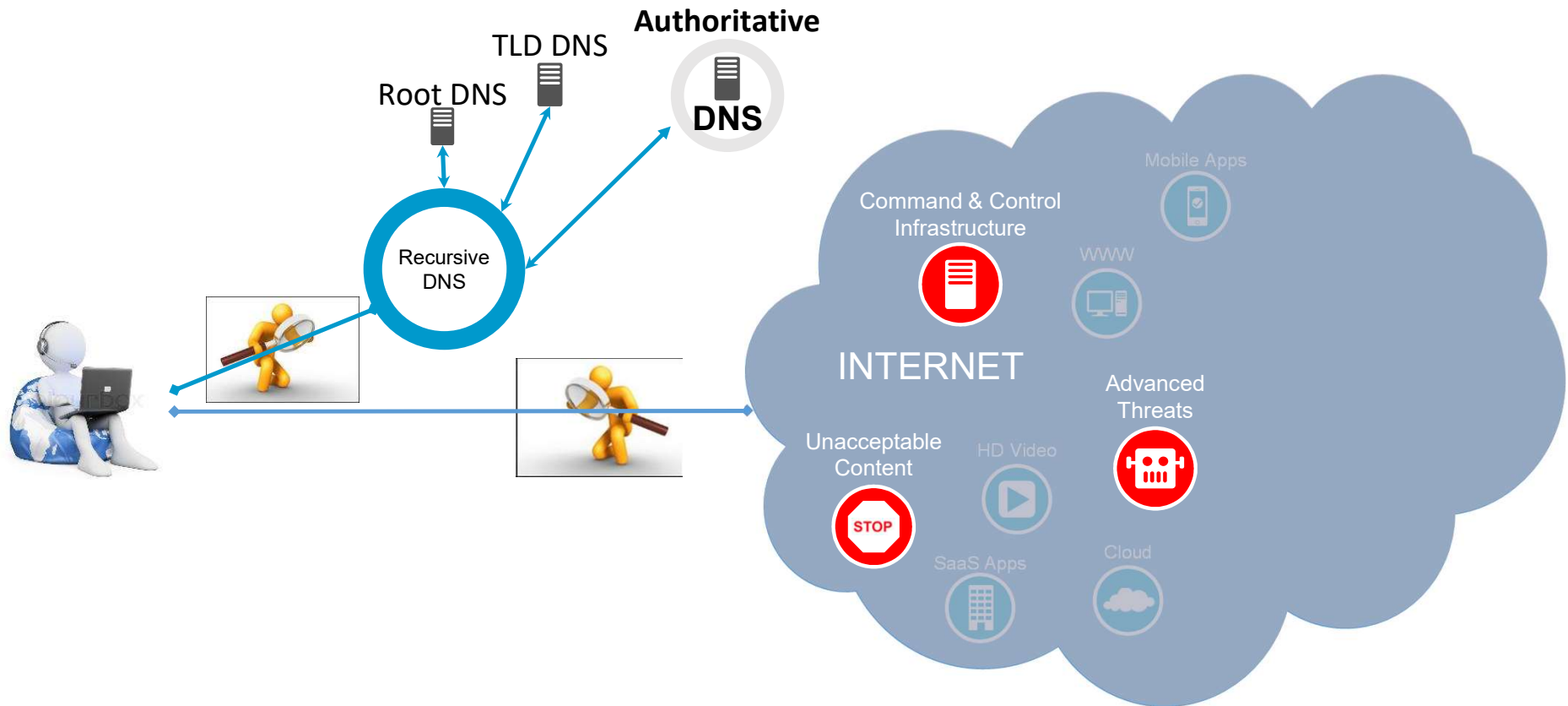
## Identity Aware Proxy

- Identity, single sign-on & multi-factor authentication
- Inline app access, app performance & app security

## Secure Internet Gateway

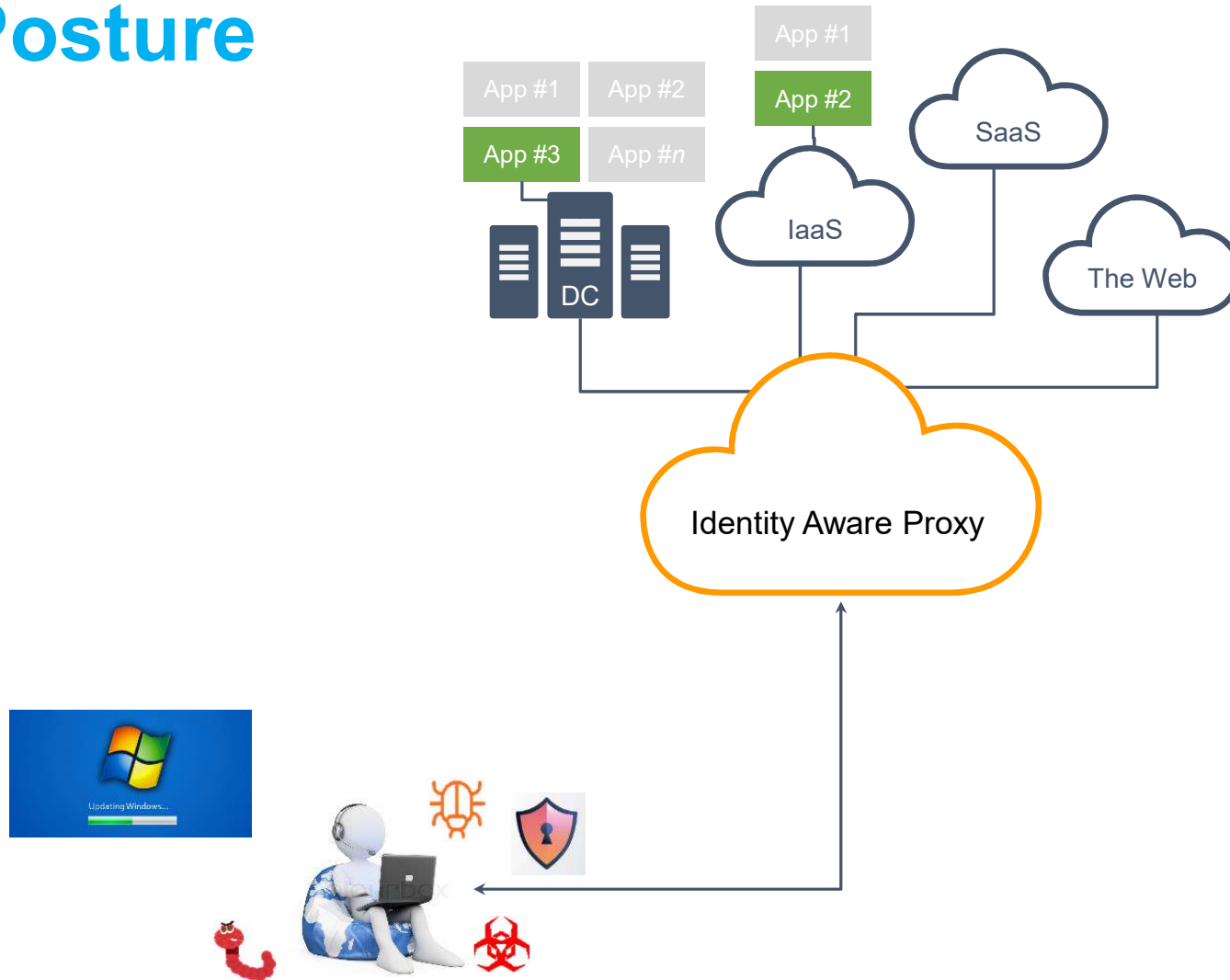
- Malware, phishing & DNS-based data exfiltration protection with inline payload analysis

# DNS-Starting Point Of Every Request





# Device Posture



## Reference architecture



Security and IT teams responsible for protecting users and providing access to corporate applications need a single set of security and access controls in order to reduce risk and scale their finite resources to meet the demands of the business.

- 1 Users access corporate applications and the web through the Akamai intelligent edge platform
- 2 Threat protection defends users from malware, phishing and malicious web content, while providing visibility to the enterprise
- 3 For corporate applications edge servers automatically drop network-layer DDoS attacks and inspect web requests to block malicious threats like SQL injections, XSS, and RFI
- 4 Identity of the user is established using on-premises, cloud based or Akamai identity stores
- 5 Based on the user's identity and other security signals, access is provided only to required applications, and not the entire corporate network
- 6 The Akamai intelligent edge platform routes authorized and authenticated users to the relevant corporate applications.

# Zero Trust Use Cases



**Virtual Backpack**

**Akamai's Zero Trust implementation**

# Value Proposition-Virtual Backpack

Simple, secure and convenient access to applications from anywhere and any device

## **Convenient**

- Seamless & consistent user experience from any device and any browser without any client software
- Reduce IT & helpdesk burden
- Consolidate and shift from heavy CAPEX to a cost effective OPEX model

## **Secure**

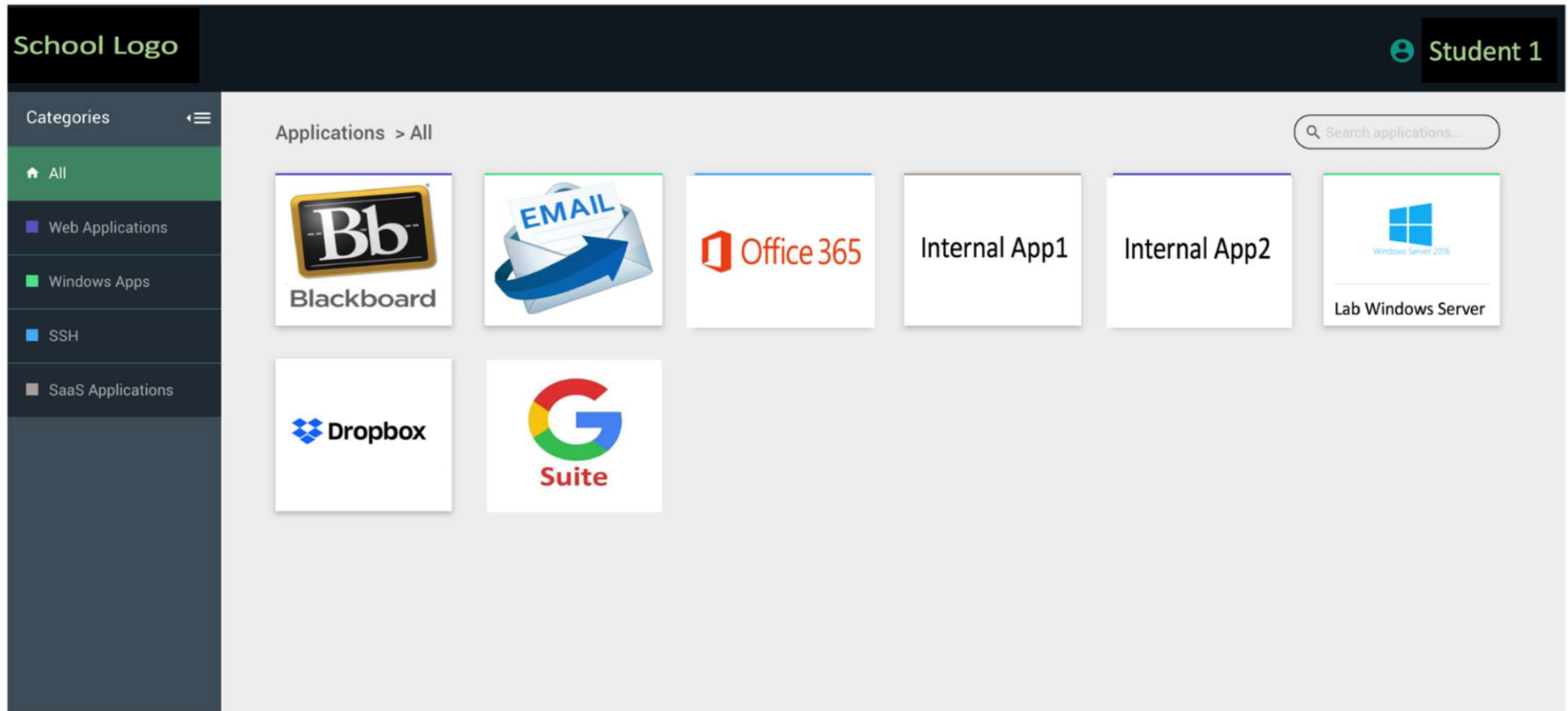
- Zero trust security model - keep remote users off your network
- Easily add MFA to any application
- Prevent threats such as Phishing, Malware, and DNS Data exfiltration

## **Visibility**

- Complete auditing and reporting of user activity
- Available as built in reports or can be integrated in with your existing tools



# Portal view after login



# Zero Trust Journey At Akamai IT

We believe a network-centric approach to security and segregation is no longer sufficient to protect our company's assets

- *“Firewalls and VPNs are great...if you don't have any users”*

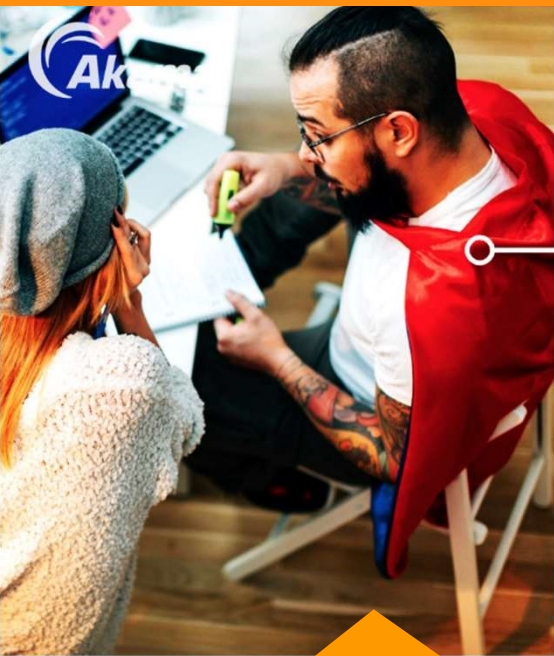
We don't trust what we don't know

We require more fine-grained access control

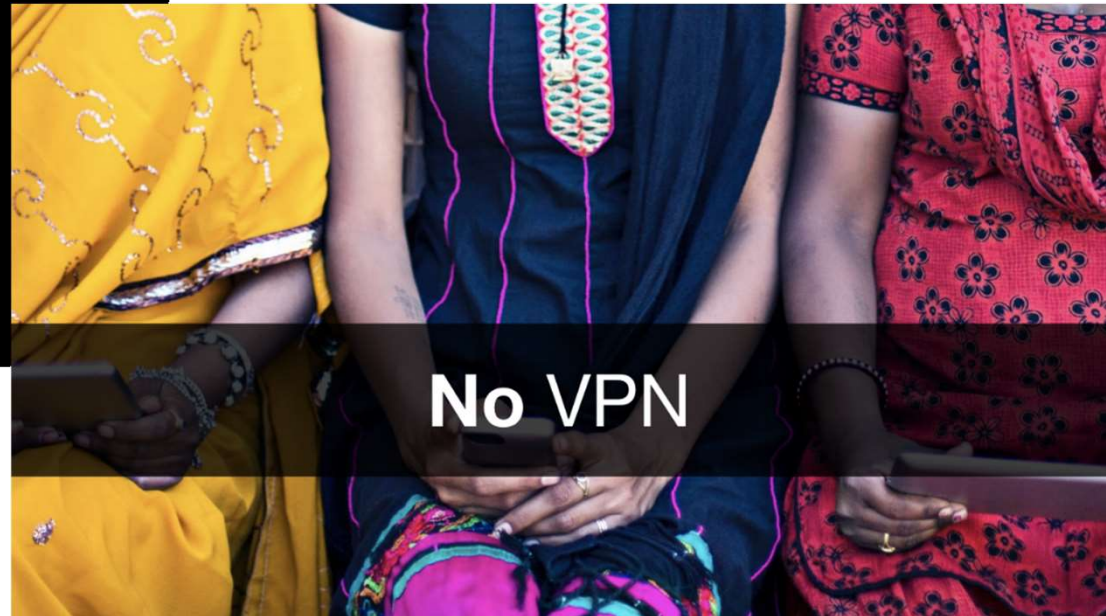
NAC was great on paper, but was too difficult and expensive to implement

We want to give our employees the same seamless and secure experience across any device from any location

# The Internet As The Corporate Network



No Inside  
No VPN  
No Passwords  
Every app seems  
like SaaS  
Every office is a  
hotspot



Akamai has always believed that  
the Internet is *THE* network

# Thank You!



 Experience the Edge



**Douglas Holland, CISSP**  
Solutions Engineer  
Public Sector, SLED  
Phone: 720.274.3924  
[dholland@akamai.com](mailto:dholland@akamai.com)